AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America
v.
James Verl Barlow

Case No. 2:21-mj-274

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of November 14, 2013 - Present in the county of Franklin in the Southern District of Ohio, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 841	Knowingly or intentionally attempt to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense a controlled substance.
21 U.S.C § 846	Attempt and conspriacy to commit an act in violation of 21 U.S.C. § 841.

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Gregory Libow, Special Agent HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: April 20, 2021

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

AFFIDAVIT

I, Gregory Libow, being duly sworn, state:

INTRODUCTION

1. I am a Special Agent with the HSI and have been since May of 2019. I am assigned to the South-Central High Intensity Drug Trafficking Area [HIDTA] Cyber Taskforce (SCHCTF) in Columbus, Ohio, where I am is responsible for conducting narcotics investigations involving dark web marketplaces. Prior to becoming a Special Agent, I was employed as a United States Customs and Border Protection (CBP) Officer for 8 years. While working for CBP, I was assigned to Columbus, Ohio and worked alongside HSI and other law enforcement agencies targeting drug and weapon shipments purchased off the internet. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Since working for HSI, I have been involved in narcotics-related arrests, executed search warrants that resulted in the seizure of narcotics, and participated in narcotics investigations. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate. In particular, I am aware that drug traffickers often communicate with their customers, couriers, and/or associates through the use of standard hardline telephones, and cellular telephones, or use of multiple telephones or other devices, to avoid detection by law enforcement.

2. I have participated in and conducted numerous investigations of violations of various state and federal criminal laws, including violations of Title 21 United States Code.

PURPOSE OF AFFIDAVIT

3. I am participating in an investigation concerning an organized group of known and unknown individuals who are suspected of involvement in criminal offenses against the United States, namely, to manufacture, distribute or dispense a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. § 846.

4. The information set forth in this affidavit is based upon my knowledge, training, experience, and participation in investigations involving the smuggling, possession, distribution, and storage of narcotics and narcotics proceeds. This information is also based on the knowledge, training, experience, and investigations conducted by fellow law enforcement officers, who have reported to me either directly or indirectly. I believe this information to be true and reliable. I know according to the Federal Analogue Act, 21 U.S.C. § 813 any chemical substantially similar to a controlled substance listed in Schedule I or II of the Drug Enforcement Administration's (DEA) Controlled Substance Schedule is to be treated as if it were listed in Schedule I, if intended for human consumption. I know is it is a violation of 21 U.S.C. § 841 to manufacture, distribute or dispense a controlled substance and a violation of 21 U.S.C. § 846 to attempt or conspire to manufacture, distribute or dispense a controlled substance.

5. The information contained in this affidavit is based upon my personal participation in this investigation, information obtained from other agents and detectives assisting in this investigation, and my review of records, documents, and other material relating to this investigation.

6. Because this affidavit is being submitted for the limited purpose of securing criminal complaints and arrest warrants, I have not included each and every fact known to me

concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that James BARLOW, Monet CARRIERE, Ronald BRUST, Matthew BARLOW, Jennifer CAMPBELL, and Tony PHAN have violated 21 U.S.C. § 841 and 21 U.S.C. § 846.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces ("DWM's"), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM's listed above, they also obtained images

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency[2]. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other

intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

e. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of April 1, 2021, one

bitcoin is worth approximately $59,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

[5] A QR code is a matrix barcode that is a machine-readable optical label.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

8. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet

FACTS ESTABLISHING PROBABLE CAUSE
SUMMARY OF THE INVESTIGATION

9. On October 04, 2019 the South-Central High Intensity Drug Trafficking Area [HIDTA] Cyber Taskforce (SCHCTF) in Columbus, Ohio, consisting of investigators assigned to HSI, Drug Enforcement Administration (DEA), United States Postal Inspection Service (USPIS) and the Internal Revenue Service (IRS), executed a federal search warrant at a Columbus Target's residence, who was using an online moniker to purchase narcotics off the Darknet site Empire Market. Investigators found and seized computers, mobile phones, media storage devices, $43,097.00 in U.S. currency, one 9mm pistol with a loaded magazine,

controlled substances and miscellaneous documents from the residence. Analysis of the Columbus Target's mobile phone, along with his Darknet Empire Market account, indicated that he had been communicating with and purchasing liquid psychedelic mushrooms from an online vendor using the Darknet moniker "TRIPWITHSCIENCE" on a regular basis.

10. Open source research determined that "TRIPWITHSCIENCE" has operated on several Darknet markets since approximately 2011, such as: Empire Market (4,719 transactions), Agora (1,500 transactions), Apollon Market (47 transactions), Berlusconi Market (60 transactions), Cryptonia Market (199 transactions), Dream Market (6,400 transactions), Tochka Market (542 transactions), Hansa Market (567 transactions), Silk Road 2.0 (2,199 transactions) and Dark Market (823 transactions) . The research also indicates that "TRIPWITHSCIENCE" may have operated on Nightmare Market, Andromeda Market, AlphaBay, Silk Road, Wall Street Market, Pandora, Black Market Reloaded, and numerous other small Darknet markets, but the number of transactions associated with those markets is unknown.

11. "TRIPWITHSCIENCE" operates primarily on Monopoly, Televend and Cannahome Darknet marketplaces selling liquid psychedelic mushrooms in 9.0 milligram/gram vials for $19.95 each. "TRIPWITHSCIENCE" specifically states how to consume the controlled substance on his marketplace listings, verifying the controlled substance analogue is for human consumption.

12. From December 23, 2019 through November 20, 2020, HSI Columbus, with the assistance from DEA and USPIS, conducted twelve controlled liquid mushroom buys from "TRIPWITHSCIENCE" via Empire and Cannahome Markets. HSI Columbus purchased a total of approximately 545 grams of liquid psychedelic mushrooms during the twelve buys.

HSI received and seized a U.S. Mail parcel associated with each buy containing suspected liquid psychedelic mushrooms. The Ohio Bureau of Criminal Investigation (BCI) Forensic Laboratory tested the contents of each parcel and determined them to be 4-Acetoxy-N,N-Dimethyltryptamine (4-AcO-DMT). This controlled substance is an analogue of 4-Hydroxy-N,N-Dimethyltryptamine (liquid psychedelic mushrooms), a schedule I controlled substance. The seized mail parcels that were shipped though U.S. Mails by "TRIPWITHSCIENCE" were shipped from U.S. Post Office blue collection boxes in the area surrounding Gulf Breeze, Florida and Memphis, Tennessee. The mail parcels consisted of United States Postal Service Priority Mail flat envelopes with Joshua Tree and Big Bend Priority Mail Stamps attached for postage. Investigators know that these types of stamps are often purchased by drug dealers using cash to remain anonymous when shipping mail parcels.

13. In October of 2020, HSI Columbus, with assistance from DEA and USPIS identified the target in Gulf Breeze, Florida mailing out the "TRIPWITHSCIENCE" parcels and executed a federal search warrant on his residence. HSI seized approximately $155,000 in cryptocurrency and cash, three firearms and approximately 22,356 grams of 4-Acetoxy-N, N-Dimethyltryptamine (4-AcO-DMT).

14. During a custodial interview with investigators, the Gulf Breeze Target stated that he was not "TRIPWITHSCIENCE" but was recruited by "TRIPWITHSCIENCE" as a reshipper to repackage and ship the vials of liquid mushrooms to "TRIPWITHSCIENCE" customers. The Gulf Breeze reshipper stated he was paid between $4,000 and $6,000 in cryptocurrency every two weeks for his services. He stated "TRIPWITHSCIENCE" had 1-3 "Order Men" working for him in Utah who would send out approximately 4-quarts of liquid

mushrooms (4-AcO-DMT) in containers concealed with a label for "Genesis Nutronics, The Natural Detox" to reshippers. The "Order Men" would also assign out the orders to reshippers and send out the names, quantity, and address for where to send the vials. The Gulf Breeze reshipper stated that he believed there were multiple reshippers working for "TRIPWITHSCIENCE" and stated when he was recruited by "TRIPWITHSCIENCE," "TRIPWITHSCIENCE" recommend he use a certain vender on Alibaba.com to buy his 10ML vials from to keep it all uniform.

15. U.S. Postal records showed the Gulf Breeze reshipper received USPS Priority Mail parcels, of approximately the same weight, that were shipped from various post offices in Salt Lake City, Sandy and Draper, Utah.

16. A U.S. Customs and Border Protection (CBP) database query revealed a subject named Tony RN is using a UPS Store Box at 3750 Hacks Cross Road Suite 102 Unit 203 in Memphis, Tennessee to receive similar 10ML vials as the Gulf Breeze reshipper, in bulk quantities, on a monthly basis. A phone number listed on one of the shipments was used to identify Tony RN as Tony PHAN who resides at 4144 Meadow Cliff Drive in Memphis, Tennessee.

17. U.S. Postal records show PHAN is receiving at least 2 USPS Priority Mail parcels from the Salt Lake City, Utah area every month to his 4144 Meadow Cliff Drive address. The parcels are the same weight as the ones that were being sent to the Gulf Breeze reshipper.

18. On October 27, 2020, HSI Memphis while conducting surveillance on PHAN, witnessed PHAN get it a Lexus GX470 bearing Tennessee license plate 757LNK and drive to a U.S. Post Offices. While wearing gloves, PHAN dropped approximately 8 packages into two different blue mail drop boxes at the location. HSI Memphis detained one of the

packages and USPIS Inspectors obtained a search warrant to open it. On October 29, 2020, USPIS Inspectors with the assistance of HSI Memphis executed the search warrant on the package and discovered thirteen 10ML vials of brown liquid. CBP Forensics Laboratory in Savannah, Georgia tested the contents of the vials and determined the liquid to be 5-hydroxy-N,N-Dimethyltryptamine, a DEA Schedule I controlled substance.

19. A subpoena issued to Coinbase, Inc. revealed throughout the life of the account, PHAN bought 10.4565797 BTC (value of $7,085.03) and received 99.87374353 BTC into the account. Records showed PHAN sold 130.236194 BTC (value of $84,195.69) from the account. Additionally, PHAN bought 4.11892993 Ethereum (ETH) (value of $628.80), received 856.8253728 ETH, and sold 653.6557839 ETH (valued at $152,568.23). Records showed PHAN received a total of seven (7) one-hop transactions from the SILKROAD2.0 and AGORA darknet markets. Records further showed PHAN's account regularly received varying amounts of crypto-currency, ranging from approximately $3,000 to $9,000, from March 5, 2017 to February 5, 2021. These received transactions occurred, on average, two times each month which aligns with the payment schedule from "TRIPWITHSCIENCE" to the Gulf Breeze reshipper.

20. On October 22, 2020, HSI Columbus received data from a seized Darknet Marketplace that contained 34 Bitcoin withdrawal wallet addresses for "TRIPWITHSCIENCE's" vender account. Using cryptocurrency analysis tracing, a Coinbase wallet was discovered sending and receiving Bitcoin from "TRIPWITHSCIENCE's" withdrawal wallets.

21. A subpoena was served to Coinbase for the subscriber information and account history associated with the Coinbase customer conducting the bitcoin

transactions. Coinbase subpoena returns revealed the user account, created on January 22, 2013, belonged to James BARLOW. The subpoena further listed BARLOW's account was a merchant account using the company name Royal Bowmen.

22. Coinbase showed BARLOW had sold approximately 312.99 Bitcoins through the exchange valued at $717,461.27 but only purchased 1 Bitcoin valued at $188.94. Similarly, BARLOW had sold both 81.11 Ethereums valued at $52,576.26 and 492.13 Litecoins valued at $30,828.25 but did not make any purchases for those cryptocurrencies on the exchange.

23. The Coinbase subpoena results showed BARLOW had vanity wallet address 1Bar1ow5zwy47N5ZkRLhvaWvVYFKT8xg8q on the account. Through cryptocurrency analysis tracing it was determined that 1Bar1ow5zwy47N5ZkRLhvaWvVYFKT8xg8q shares private keys with vanity address 1TWS1XtNX9pwjWJSxnRarqiZhYWRHoUWs. 1TWS1XtNX9pwjWJSxnRarqiZhYWRHoUWs is believed to be a possible second vanity wallet for "TRIPWITHSCIENCE", also known as TWS. A 2015 Reddit post showed "TRIPWITHSCIENCE" used the vanity wallet 1Trip1V2s5cbDeFjCLeJQEvRgT7T7Jy3k.

24. While conducted crypto-currency analysis on the bitcoin wallet addresses listed in the Coinbase subpoena for BARLOW, investigators discovered five (5) direct transactions, from November 20, 2013 to September 2, 2014, between BARLOW and "TRIPWITHSCIENCE's" darknet withdraw wallets. Investigators commonly observe darknet vendors withdraw their drug proceeds directly into their personal accounts when they first begin selling on the darknet.

25. According to the BARLOW's Coinbase subpoena results, on July 15, July 18, August 15, and September 6 of 2016, BARLOW used his Coinbase account, via

Shiftpayments, to make six purchases from Thomas Scientific Inc. A clear web search of Thomas Scientific Inc revealed a website THOMASSCI.COM which sells numerous laboratory supplies, chemicals, instruments, and equipment.

26. On December 14, 2016, BARLOW used his Coinbase account, via Shiftpayments, to make a purchase at "Sticker Mule." A clear web search of Sticker Mule revealed a website STICKERMULE.COM which sells custom labels and stickers. It is believed that BARLOW could have used Sticker Mule to make the Genesis Nutronics labels used by the "Order Men."

27. On April 24, 2017, BARLOW used his Coinbase account, via Shiftpayments, to make a purchase from FCD*Freund Container. A clear web investigative search revealed Freund Container is now Berlin Packaging which sells food, beverage, and pharmaceutical containers. Several containers found on the website match the container sent by the "Order Men" in Utah to the Gulf Breeze reshipper that was found during the search warrant.

28. A U.S. Customs and Border Protection database query of international parcel seizures revealed three possible seizures associated with BARLOW. One of those seizures was 113 grams of 4-Acetoxy-N, N-Dimethyltryptamine (4-AcO-DMT) addressed to Jim BARLOW. The other two were 105 grams of 3,4-Methylenedioxymethamphetamine (MDMA) addressed to a James BARLOW and 1,416 grams of Gamma Hydroxy Butyrate (GHB) addressed to a "Adam Businger" at James BARLOW's residence, 1409 Bonita Avenue February 7, 2019.

29. A public record check showed the company Nutra HQ was registered to the P.O. BOX 29502 #61122 in Las Vegas, Nevada and listed the managing member of the company to be James Barlow at 1409 Bonita Ave in Las Vegas, Nevada.

30. A CBP database query of international shipments showed Nutra HQ had three international shipments. Two shipments were sent to a virtual office space in Las Vegas, Nevada containing a grinding machine (October 20, 2017) and 2500 10ML plastic bottles (June 30, 2020). A third shipment to Nutra HQ was to the same virtual office space company but to a location in Salt Lake City, Utah. This shipment was also for 2500 plastic bottles (June 30, 2020) and was sent from the same shipper who sent 10ML bottles to the Gulf Breeze reshipper to prepare and distribute liquid mushrooms (4-AcO-DMT) for "TRIPWITHSCIENCE."

31. On November 11, 2017. USPIS discovered a USPS account with the username NutraHQ registered to a James BARLOW. This online USPS account revealed that from October 19, 2018 to June 24, 2020, approximately five (5) orders of Priority Flat Rate Envelopes and about twenty-six (26) orders for at least $300 each of Priority Flat Rate stamps (Big Bend Stamps) were made. Law enforcement knows that these Priority Flat Rate stamps are most commonly used among Darknet vendors, and are the stamps found to be used by all known "TRIPWITHSCIENCE" reshippers to date.

32. Further crypto-currency tracing conducted on wallet addresses belonging to "TRIPWITHSCIENCE" that were received from seized darknet marketplace data showed that on June 15, 2017, a second Coinbase account received bitcoin from "TRIPWITHSCIENCE." Results from a subpoena served to Coinbase revealed this account belonged to Monet Latrice CARRIERE. The account showed CARRIERE received 334.47112423 BTC, sent 6.29361 BTC, and sold 327.5485325 BTC (valued at $304,392.12) during the life of the account. Additionally, CARRIERE transacted smaller amounts of BitcoinCash, Bitcoin Satoshi Version, Ethereum, and LiteCoin through the account.

33. The Coinbase subpoena on CARRIERE's account also revealed that from October 30, 2018 to April 10, 2019, CARRIERE had notable transactions from CAPSULE CONNECTION, LLC, FREUND CONTAINER A DIV BE, SPICE JUNGLE, LLC, and 22 purchases from USPS.COM POSTAL STORE. Total purchases from the USPS.COM POSTAL STORE equaled $21,184.96.

34. A CBP database query of international packages revealed CARRIERE had received 11 shipments of plastic bottles, between 2014 through 2017, matching the description of the bottles PHAM and the Gulf Breeze reshipper were receiving to package "TRIPWITHSCIENCE's" orders.

35. A subpoena served to Capsule Connection, LLC revealed CARRIERE was associated with six (6) orders of bulk "Gelatin Capsules". These capsules were purchased from February 12, 2019 to November 17, 2020 and encompassed 279,000 gelatin capsules. The size and shape of these capsules match capsules sold by darknet vendor PERFECTSHROOMS.

36. Freund Container, now a division of Berlin Packaging LLC, was issued a subpoena for the account history associated with James BARLOW, Monet CARRIERE and NUTRA HQ. Berlin Packaging LLC subpoena return revealed 11 orders from March 24, 2018 through November 18, 2020. The first two orders were shipped to James BARLOW at 1409 Bonita Avenue in Las Vegas, Nevada. The next 7 orders were shipped to Monet CARRIERE at her residence in Las Vegas, Nevada and the last two orders, on June 16, 2020 and November 18, 2020 were shipped to Nutra HQ/Monet Carriere at 4001 S 700 E, Suite 500 in Salt Lake City, Utah. The last 5 orders consisted of Item number 3211B15 that matched the bottles found at the residence of the Gulf Breeze reshipper, on October 20, 2020

with a "GENESIS NUTRONICS" label. Per Gulf Breeze reshipper, these bottles were supplied to him from "TRIPWITHSCIENCE" and were suspected to contain liquid psilocybin mushrooms. Per Berlin Packaging's website, these bottles are described as "84 oz Natural HDPE Plastic Kautex Wide Mouth UN-Rated Leakproof Bottles (Blue Tamper-Evident Cap) - 3211B15" and are similar in shape, color, and size to the bottles "TRIPWITHSCIENCE" mailed to his reshippers

37. Postal records show the Gulf Breeze reshipper and Tony PHAN, both received an average of 2-4 parcels containing 4-8 bottles suspected of containing approximately 84 ounces of concentrated liquid psilocybin mushrooms monthly from "TRIPWITHSCIENCE." This coincides with the 268 bottles BARLOW and CARRIERE ordered and the amount the Gulf Breeze reshipper and PHAN received which is estimated to be 252 bottles (average of 6 bottles a month for 21 months totaled for both reshippers).

38. On November 30, 2020 Spice Jungle LLC was issued a subpoena for the account history associated with Monet CARRIERE, James BARLOW, NUTRAHQ and any customers using the shipping address of 4001 South 700 East, Suite 500, Salt Lake City, Utah 84017. On December 7, 2020, Spice Jungle LLC subpoena returns revealed numerous orders, totaling $8,429,51, associated with CARRIERE, James BARLOW, Matt BARLOW, Jenni CAMPBELL and NUTRAHQ between the July 2, 2017 and November 5, 2020.

39. Since October 21, 2020, USPIS Inspectors have been able to obtain approximately eight (8) U.S. Post Office surveillance videos of the Salt Lake City, Utah targets sending parcels to PHAN and the Gulf Breeze reshipper. The surveillance videos consisted of three (3) videos of a female and five (5) videos of a male dropping off USPS Priority Mail parcels at the service counter and paying cash. A clear web search of associates

of James BARLOW, identified the targets as Matthew BARLOW, James BARLOW's younger brother and Jennifer CAMPBELL, Matthew BARLOW's roommate and suspected girlfriend.

40. A public record check of address 4001 South 700 East, Suite 500, Salt Lake City, Utah revealed the address came back to Avanti Workspace, a virtual office company. Avanti Workspace subpoena returns showed the virtual office of NUTRAHQ/BARLOW had four parcels awaiting pickup from Spice Jungle LLC, Capsule Connection LLC, and Berlin Packaging LLC. On December 7, 2020 Avanti Workspace stated that on December 4, 2020, the packages had been picked up by a male with "rainbow colored hair" and a female near of the close of day. On December 8, 2020 investigators provided an employee of Avanti Workspace with a photograph of Matthew BARLOW and Jennifer CAMPBELL. The employee confirmed that it was Matthew BARLOW and CAMPBELL who picked up the packages for NUTRAHQ on December 4, 2020.

41. A subpoena issued to Coinbase, Inc. revealed Matthew BARLOW created an account on February 21, 2018. Jennifer CAMPBELL was also listed as being associated with the account. Throughout the life of the account, Matthew BARLOW and CAMPBELL's account received 22.72432712 BTC, bought 0 BTC, sent 0.54636692 BTC, and sold 22.05309677 BTC (valued at $168,692.62). Analysis of the account determined Matthew BARLOW and CAMPBELL would regularly receive various amounts of Bitcoin into the account and then withdraw these funds in U.S. Currency to his bank account. Investigators conducted blockchain analysis on the incoming transactions and determined many of the funds were received from Wasabi Mixing Service, a service used to conceal origins of a transaction. In an image Matthew BARLOW provided to Coinbase to verify his

identity, Matthew BARLOW can be seen standing in the picture holding a temporary driving permit. In the background of this image, multiple USPS Priority Mail shipping boxes appear to be stacked on a cabinet. These boxes match the boxes of suspected drugs being sent from the Salt Lake City, Utah area to PHAN and the Gulf Breeze reshipper.

42. On or about January 19, 2021, HSI SAs at the Salt Lake City, Utah office initiated surveillance of Matthew BARLOW at his residence of 6431 S 725 E Street in Murray, Utah. At approximately 17:30 hours, HSI SAs witnessed Matthew BARLOW leave his house and drive to a U.S. Post Office in Sandy, Utah. HSI SAs witnessed Matthew BARLOW give the Postal employee behind the counter three USPS International Priority Mail parcels and pay for the shipment using cash. Matthew BARLOW collected his receipt and then returned back to his residence.

43. A Postal database query conducted by USPIS determined the three parcels, CH123337788US, CH123338050US and CH123338240US, sent by Matthew BARLOW were addressed to Daniel BARWELL at 14 Vulcan Cresecent, Scawsby, Doncaster, DN5 8WA, United Kingdom. All three parcels contained a fictitious return address of Nathan Coleson, 10075 S Kimsbrough Road, Sandy, Utah. Each parcel had $77.35 of postage affixed, were manifested as a “cleanse”, and valued at $35. The weight of each package was approximately the same weight of packages sent to PHAN and the Gulf Breeze reshipper.

44. While reviewing seized Darknet Marketplace data from “TRIPWITHSCIENCE,” HSI SAs discovered messages between “TRIPWITHSCIENCE and Darknet moniker “DARKLOIS.” The messages identified “DARKLOIS” as a shill account created by “TRIPWITHSCIENCE” to promote his business and create test shipments on his account. SAs discovered a similar conversation between “DARKLOIS” and Darknet vendor

"PERFECTSHROOMS," the only other account "DARKLOIS" reviewed and interacted with.

45. PerfectShrooms currently has listings Televend, Monopoly and Cannahome marketplaces. The account has listings for 3.5 grams to 114 grams of "Organic Mushrooms" (Psilocybe Cubensis Shrooms) in capsule form. A February 14, 2020, Established Vender Application[7] states PerfectShrooms has processed 7,800 orders on 15 different darknet marketplaces.

46. On November 30, 2020 HSI Columbus, with the assistance of DEA and USPIS conducted a controlled buy for 7 grams of powdered psilocybin mushroom capsules from "PERFECTSHROOMS" via Monopoly Market. Due to shipping delays, "PERFECTSHROOMS" sent a second parcel of 7 grams of powered psilocybin mushroom capsules. Both parcels were seized, tested at Ohio BCI Forensics Laboratory, and determined to be 4-Acetoxy-N,N-Dimethyltryptamine (4-AcO-DMT). The first parcel contained a return address in Midvale, Utah and the second contained a returned address in Memphis, Tennessee.

47. On or about January 4, 2021, HSI Columbus received electronic results from a search warrant issued to Google for records associated with Jim.V.Barlow@Gmail.com. In the records, images showed containers and bags of mushrooms with the cartoon scientist icon of "TRIPWITHSCIENCE" and the script "u/TripWithScience" written underneath. The multiple images appeared to show a step-by-step alcohol extraction of psilocybin mushrooms

[7] Established Vendor Applications are used by vendors applying to new marketplace places. Vendors will list the markets they have sold on and how many transactions they've completed in an attempt to get discounted or waived vendor fees.

next to the "TRIPWITHSCIENCE" icon and the script "u/TripWithScience". Metadata[8] in the images showed they were taken at 1345 Hawaiian Hills Ave., Las Vegas, Nevada 89183 on November 16, 2020. Images were found of mushrooms growing on substrate. In the images, the words "PerfectShrooms" with cartoon mushrooms were printed on a piece of paper next to the growing mushrooms. The metadata of both images showed they were taken on November 15, 2020 near 1345 Hawaiian Hills Avenue., Las Vegas, Nevada 89183.

48. A clear web search of 1345 Hawaiian Hills Avenue shows the residence is occupied by Ronald Royal Edwards BRUST. BRUST co-owns the business Illuminated Couture and Good-To-Glow with James BARLOW.

49. A video found in the results of the search warrant served to Google, shows an individual believed to be Ronald BRUST. In the video the male narrated how he dried horse manure and then showed how to sift the manure to use it for "mushroom cultivation". The individual, believed to be BRUST, stated the manure was "sun dried in Las Vegas weather" and stated, "It's quite a bit of a process and that is what goes into making magic mushrooms". The metadata of the video showed it was taken September 23, 2020. Distinctive tattoos on the arm and foot of the individual in the video match tattoos observed on photographs showing the arm of BRUST in a Facebook post on November 17, 2018. In a separate image an individual holding a large bag of gelatin capsules filled with a

[8] Image metadata is text information pertaining to an image file that is embedded into the file or contained in separate file that is associate with it. Image metadata includes details relevant to the image itself as well as information about its production. Automatically generated metadata can include the camera brand and model, the date and time when the image was created and the GPS location where it was created.

light brown powder can be seen. A tattoo on the foot of the individual holding the bag of capsules match the tattoo on the foot of the individual in video "8aa6fb92-ffc7-4257-8d0b-02e7f72b9493.mp4", both believed to be BRUST's left foot. The capsules are congruent with the capsules sold by "PERFECTSHROOMS."

50. A subpoena issued to Coinbase, Inc. revealed BRUST possessed a personal and a business account. During the life of the personal account, BRUST bought 0.02280327 BTC (valued at $190), received 5.4995289 BTC, and sold 5.45251994 BTC (valued at $63,117.73). Investigative analysis was conducted on the wallet addresses of BRUST's personal account. Analysis showed one three-hop transaction between a bitcoin mixer and BRUST. During the life of the business account, BRUST bought 0 BTC, received 26.39784414 BTC, and sold 27.02296321 BTC (valued at $37,810.89). Investigative analysis was conducted on the wallet addresses of BRUST's business account. Analysis showed BRUST received two (2) four-hop transactions from the WALL ST and HYDRA darknet markets respectively on January 19, 2019. Further, BRUST received 1.38475291 BTC (valued at $5,118.10) on January 19, 2019 from a wallet which also sent funds to a second co-conspirator.

51. While analyzing James BARLOWS Google Drive search warrant results investigators found several photos and videos depicting James BARLOWS illicit drug use, the photos include drugs believed to be DMT, Ketamine, LSD, MDMA and Psychedelic Mushrooms. Investigators also found a spreadsheet named TCS Accounting that tabs listing from 2014-2021, each tab appeared to show an income and expense table that included multiple transactions with descriptions with reference to Darknet Marketplaces, drugs, known "TRIPWITHSCIENCE reshipper code names, reimbursement for materials used by

the reshippers (vials, Everclear, refrigerators and stamps), bitcoin mixing services and TWS Charity, which appears to be a direct reference to "TRIPWITHSCIENCE's" donation wallet. The spreadsheet shows an average yearly income of $211,019.52 in 2014 and raising to a yearly income of $2,814,606.25 by 2021. The spreadsheet showed James BARLOWS value as $4,378,974.48 in 2020.

52. In the Google Drive search warrants results was a spreadsheet titled "2015 TCS Accounting." In the spreadsheet were 9 tabs, 7 of the tabs were titled 2015 and known two letter abbreviations for darknet markets AlphaBay, Nucleus Market, Abraxas Market, MiddleEarth Marketplace, Evolution Market, Agora Market and Black Bank Market. Each tab listed multiple transactions that included a date, time, a notation that payment was received and blockchain transaction hash. HSI Columbus ran several of the bitcoin blockchain transaction hashes and results came back corresponding Darknet marketplace reference in the tab title. A tab titled "2015 Received" appeared to list all 704 Darknet transactions from January 1, 2015 through December 9, 2015 indicting a net of $401,816.78.

53. In the Google Drive search warrant results was a spreadsheet titled "archived rbow btc addresses" showed 500 bitcoin wallet addresses, several the addresses has descriptions next the address that included: "from tws," "pay 9-15 from tws," "from trip," "from tws through bitmixer," "from lois evo," "from AG loisdark," "August SR" and "Evolution July."

54. On James BARLOW's Google Drive was a folder titled "DNM," which is known to law enforcement as an abbreviation for Darknet Market. The folder 7 files including a spreadsheet named "4AC Sources" that listed several websites believed to sale 4-AcO DMT. The spreadsheet included the price, price per gram and whether or not they accepted bitcoin.

Another spreadsheet found in the "DMN" folder was titled "Fulfiller Recurring Expenses" which listed cost for stamps, gloves, bubble wrap, vials, vacuum bags, printer paper, mailing labels and misc. A third spreadsheet titled "TWS Sales Summation" included 7 tabs. On the first tab titled "Sheet 1" is a list of Silk Road, Agora and Evolution Darknet markets orders, order per day, number of vials, vials per day and vials ordered for the month of July. The sheet goes on to break down the cost per gallon to mix 2.8 liters of Everclear, 11.5 grams of 4-AcO DMT and juice. On the tab titled "AG July" shows a ledger of sales from Agora Market that include quantity of Liquid Mushrooms order, events, status of order and the feedback left by the customer. A word document titled "MVI_1537_Packaging" is a 6-page word documents that describe in great detail the advised process of packaging and shipping the vials. A fourth spreadsheet titled "Mo Timesheet" listed hours Mo, a nickname used for Monet CARRIERE worked from September 2, 2014 to September 30, 2014. The spreadsheet listed CARRIERE's "salary" as $2000 and listed two "commissions", one for $1,730 and one for $1,890. The spreadsheet further listed "Stamp/Supply" reimbursements for $1,845 and $2,212.50. Investigators also found a screenshot of a text message from CARRIERE in another folder on the Google Drive, the text message was from CARRIERE asking James BARLOW if they could do the "vial" count tonight so she could close the spreadsheet.

55. Due to the evidence provided above, it is believed that James BARLOW is the head of the "TRIPWITHSCIENCE' and "PERFECTSHROOMS" Drug Trafficking Organization (DTO). It is believed that Monet CARRIERE began as a reshipper for "TRIPWITHSCIENCE" and now handles the ordering of precursors needed for mixing the liquid and powdered mushrooms sold by the DTO. Investigators believe Matthew BARLOW and Jennifer CAMPBELL mix the liquid mushrooms in quart bottles that they ship to Tony

PHAN in Memphis, Tennessee, and Daniel BARWELL in the United Kingdom. Tony PHAN then repackages the quarts bottles of liquid mushrooms into vials and ships them to "TRIPWITHSCIENCE" customers inside the United States. Daniel BARWELL does the same thing as PHAN for all "TRIPWITHSCIENCE" customers outside the United States. Ronald BRUST is believed by investigators to be growing psilocybin mushrooms for the DTO. Investigators also believe BRUST assist with packaging of capsules "PERFECTSHROOMS" and marketing for the darknet listings.

56. This summation does not include all duties of the DTO members and is only meant to serve as a general outline. It is the belief of investigators that the duties of the DTO members change with the needs of the organization.

CONCLUSION

57. Based on the foregoing facts, I believe that there is probable cause that James BARLOW, Monet CARRIERE, Ronald BRUST, Matthew BARLOW, Jennifer CAMPBELL and Tony PHAN are attempting and conspiring to manufacturing, distributing or dispensing a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. §846. Accordingly, I request the issuance of a criminal complaint and arrest warrant for James BARLOW, Monet CARRIERE, Ronald BRUST, Matthew BARLOW, Jennifer CAMPBELL, and Tony PHAN.

58. I further request that due to the ongoing nature of this investigation, the application, search warrant, and this affidavit be sealed until further ordered of the Court in order to avoid premature disclosure of the fact of this investigation and the information contained in this affidavit.

Special Agent Gregory Libow

Homeland Security Investigations

April 20, 2021

Subscribed and sworn to before me this ____ day of _____, 2021.

Kimberly A. Johnson
United States Magistrate Judge